AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior listings of claims in the application:

1. (currently amended): An electronic data storage system comprising:

a file device for storing at least electronic data; and

a data processing unit which

generates a first check ~~codes~~ code for detecting falsification ~~respectively for~~ of said electronic data and a second check code for detecting falsification of a public key-based electronic signature using a secret encryption method and/or an encryption key when the electronic data is registered,

stores said electronic data, said public key-based electronic signature, and said ~~respective~~ first and second check codes into said file device,

respectively verifies the validity of said stored electronic data and said electronic signature using said first and second check codes attached to the stored electronic data and said electronic signature when said electronic data is output, and then

accesses said electronic data and said electronic signature when said validity is confirmed,

wherein said data processing unit generates said first and second check codes by a method unique to said system, and

verifies the validity of said stored electronic data and said electronic signature by creating a third check code from said electronic data and a fourth check code from said electronic signature by said method unique to said system, and comparing said stored first check code with said third check code and said stored second check code with said fourth check code.

2. (currently amended): An electronic data storage system comprising:

a file device for storing at least electronic data; and

a data processing unit which

generates a check code for detecting falsification for a public key-based electronic signature using a secret encryption method and/or an encryption key when said electronic data is registered,

stores said electronic data, said public key-based electronic signature and the falsification check code for said electronic signature into said file device,

verifies the validity of said electronic signature using the check code attached to said electronic signature and

verifies the validity of said electronic data using said electronic signature when said electronic data is output, and then

accesses said electronic data and said electronic signature when said validity is confirmed,

wherein said data processing unit generates said check code by a method unique to said system, and

verifies the validity of said stored electronic data by creating a second check code from said electronic signature by said method unique to said system, and comparing said stored check code with said second check code.

3. (currently amended): The electronic data storage system according to Claim 1, wherein said data processing unit outputs said electronic data, ~~with attaching~~ the public key-based

electronic signature, and a second public key-based electronic signature created at access to the public key-based electronic signature ~~at registration to be accessed~~ after verifying the validity of said electronic data and said electronic signature.

4. (currently amended): The electronic data storage system according to Claim 1, wherein said data processing unit outputs said electronic data, ~~with attaching~~ the public key-based electronic signature and a second public key-based electronic signature created at access to the electronic data ~~to be accessed~~ after verifying the validity of said electronic data and said electronic signature.

5. (currently amended): The electronic data storage system according to Claim 2, wherein said data processing unit outputs said electronic data, ~~with attaching~~ the public key-based electronic signature and a second public key-based electronic signature created at access to the public key-based electronic signature ~~at registration to be accessed~~ after verifying the validity of said electronic data and said electronic signature.

6. (currently amended): The electronic data storage system according to Claim 1, wherein said data processing unit stores a certificate of the public key with which said electronic signature was created, simultaneously along with said electronic signature into said file device, when said electronic signature is created.

7. (currently amended): The electronic data storage system according to Claim [[1]] 6, wherein said data processing unit stores or outputs the expiration information of said public key certificate simultaneously.

8. (currently amended): The electronic data storage system according to Claim 2, wherein said data processing unit stores [[the]] a certificate of the public key with which said electronic signature is created, simultaneously along with said electronic signature into said file device, when said electronic signature is created.

9. (currently amended): The electronic data storage system according to Claim [[2]] 8, wherein said data processing unit stores or outputs the expiration information of said public key certificate simultaneously.

10. (currently amended): The electronic data storage system according to Claim 1, wherein said data processing unit creates a pair of said public key and said secret key according to [[the]] a request for key creation, issues [[the]] a request of issuing [[said]] a public key certificate to a CA office, acquires [[said]] a public key certificate, and stores said acquired public key certificate in said file device.

11. (currently amended): An electronic data storage method comprising:

a step of ~~respectively~~ generating a first check ~~codes~~ code for detecting falsification [[for]] of electronic data and a second check code for detecting falsification of a public key-based

electronic signature using a secret encryption method and/or an encryption key, when said electronic data is registered;

a step of storing said electronic data, said public key-based electronic signature, and said ~~respective~~ first and second check codes into a file device;

a step of respectively verifying the validity of said stored electronic data and said electronic signature using said first and second check codes attached to said stored electronic data and said electronic signature when said electronic data is output from said file device; and

a step of accessing said electronic data and said electronic signature when said validity is confirmed,

wherein said generating step comprises a step of generating said first and second check codes by a method unique to said system, and wherein said verifying step comprises:

a step of creating a third check code from said electronic data and a fourth check code from said electronic signature by said method unique to said system; and

a step of comparing said stored first check code with said third check code and said stored second check code with said fourth check code.

12. (currently amended): The electronic data storage method according to Claim 11, further comprising a step of outputting said electronic data, ~~signature at registration with attaching a~~ the public key-based electronic signature, and a second public key-based electronic signature created at access to the public key-based after verifying the validity of said electronic data and said electronic signature.

13. (currently amended): An electronic data storage method, comprising:

a step of generating a check code for detecting falsification [[for]] of a public key-based electronic signature using a secret encryption method and/or an encryption key, when said electronic data is registered;

a step of storing said electronic data, said public key-based electronic signature, and said falsification check code for said electronic signature into a file device; and

a step of verifying the validity of said electronic data ~~using said electronic data~~ using said electronic signature after verifying the validity of said electronic signature using the check code attached to said electronic signature when said electronic data is output from said file device, and then accessing said electronic data and said electronic signature when said validity is confirmed,

wherein said generating step comprises a step of generating said check code by a method unique to said system,

and wherein said verifying step comprises:

a step of creating a second check code from said electronic signature by said method unique to said system; and

a step of comparing said stored check code with said second check code.

14. (currently amended): The electronic data storage method according to Claim 13, further comprising a step of outputting said electronic data, ~~signature with attaching a~~ the public key-based electronic signature and a second key-based electronic signature created at access to the public key-based electronic signature after verifying the validity of said electronic data and said electronic signature.

15. (currently amended): The electronic data storage method according to Claim 13, ~~wherein output step comprises~~ further comprising a step of outputting said electronic data, ~~with attaching a~~ the public key-based electronic signature and a second key-based electronic signature created at access to the public key-based electronic signature after verifying the validity of said electronic data and said electronic signature.

16. (currently amended): The electronic data storage method according to Claim 11, wherein said storage step comprises a step of storing a certificate of the public key with which said electronic signature was created, simultaneously along with said electronic signature into said file device, when said electronic signature is created.

17. (currently amended): The electronic data storage method according to Claim [[13]] 16, wherein said storage step comprises a step of storing a certificate of the public key with which said electronic signature was created, simultaneously along with said electronic signature, when said electronic signature is created.

18. (currently amended): The electronic data storage method according to Claim 11, wherein said storage or output step comprises a step of storing or outputting the expiration information of [[said]] a public key certificate simultaneously.

19. (currently amended): The electronic data storage method according to Claim 11, further comprising:

a step of creating a pair of said public key and said secret key according to [[the]] a request for the key creation; [[,]]

a step of issuing [[the]] a request of issuing [[said]] a public key certificate to a CA office; and [[,]]

a step of acquiring said public key certificate, and storing said public key certificate in said file device.

20. (currently amended): The electronic data storage method according to Claim 13, wherein said storage or output step comprise a step of storing or outputting the expiration information of [[said]] a public key certificate simultaneously.

21. (currently amended): The electronic data storage method according to Claim 13, further comprising:

a step of creating a pair of said public key and said secret key according to [[the]] a request for the key creation; [[,]]

a step of issuing the request of issuing [[said]] a public key certificate to a CA office; and [[,]]

a step of acquiring said public key certificate, and storing [[same]] said public key certificate in said file device.